
# Declarația Politicilor si Practicilor de Certificare

| EMISA DE: | | |
|---|---|---|
| **DEPARTAMENT** | **NUME** | **DATA** |
| MANAGEMENTUL POLITICILOR SI PROCEDURILOR | Ofițer de Securitate IT | 24/04/2017 |

| APROBATA DE: | | |
|---|---|---|
| **DEPARTAMENT** | **NUME** | **DATA** |
| COMITETUL DE MANAGEMENT AL POLITICILOR SI PROCEDURILOR | DIRECTOR TEHNIC | 28.04.2017 |

| ISTORICUL MODIFICARILOR: | | | |
|---|---|---|---|
| **VERSIUNE** | **AUTOR** | **DETALII MODIFICARI** | **DATA:** |
| 1.0 | Ofițer de Securitate IT | Publicarea primei versiuni a documentului | 28.04.2017 |
| 1.1 | Director Tehnic | Revizuire document | 31.01.2020 |
| 1.2 | Director Tehnic | Revizuire document | 31.01.2021 |
| 1.3 | Director Tehnic | Revizuire document | 30.06.2023 |

| | | | |
|---|---|---|---|
| 1.4 | Director Tehnic | Completări secțiune 3.1 Cererea unui certificat calificat | 31.10.2023 |
| 1.5 | Director Tehnic | Actualizare secțiune 3.1 Cererea unui certificat calificat – Anexa Reguli validare cerere certificate digital calificat | 28.02.2025 |
| 1.6 | Ofițer de Securitate IT | Actualizare document conform prevederilor din Legea 214/2024 | 06.10.2025 |
| | | | |
| | | | |
| | | | |

# Cuprins

# Termeni si definiții

| | |
|---|---|
| Acces | Posibilitatea utilizării unei resurse informationale pe baza unui drept dobândit |
| Administrator | Utilizator care este autorizat de a folosi conturi administrative sau privilegiate pentru a-si indeplini sarcinile de serviciu. In general, administratorul are dreptul de gestiune asupra celorlalte tipuri de utilizatori. |
| Angajat | Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de munca semnat. |
| Autentificare | Validarea identitatii unui utilizator sau a unei entitati. Procesul autentificarii verifica daca entitatea este cea care pretinde a fi si in functie de rezultatul obtinut ofera sau nu acces catre resursele solicitate. |
| Autoritatea de Certificare | Institutie de incredere care emite certificate aferent cererilor eligibile. Pentru acest proces, Autoritatea de Certificare verifica informatiile specificate de solicitant in cererile de emitere a certificatului. |
| Autoritatea de Inregistrare | Institutie care este responsabila cu identificarea si autentificarea subiectului unui certificat |
| Cerere de emitere a unui certificat | Document electronic care contine detalii cu privire la certificatele care urmeaza sa fie create de catre Autoritatea de Certificare si inregistrate de catre Autoritatea de Inregistrare |
| Certificat | Colectie de date in forma electronica ce atesta legatura dintre datele de verificare a semnaturii electronice si o persoana, confirmând identitatea acelei persoane |
| Certificat calificat | Certificat eliberat de un furnizor de servicii de certificare in conditiile prevazute de Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea, si |

| | |
|---|---|
| | ale Regulamentului (UE) nr. 910/2014 privind identificarea electronica si serviciile de încredere pentru tranzacțiile electronice pe piata interna |
| Certificat digital | Reprezinta un act de identitate sub forma electronica folosit pentru autentificarea si certificarea identitatii unui utilizator in cazul accesarii de la distanta a unor resurse. |
| Certificat revocat | Certificat de cheie publica inclus in Lista Certificatelor Revocate |
| Certificat valid | Certificat de cheie publica emis de catre o Autoritate de Certificare, acceptat de solicitant si care nu a fost supus procesului de revocare |
| Cheie privata | Un cod digital cu caracter de unicitate, generat printr-un dispozitiv hardware si/ sau software specializat. In contextul semnaturii digitale, cheia privata reprezinta datele de creare a semnaturii electronice, asa cum apar ele definite in lege |
| Cheie publica | Cod digital, perechea cheii private necesara verificarii semnaturii electronice. In contextul semnaturii digitale cheia publica reprezinta datele de verificare a semnaturii electronice, asa cum apar ele definite in lege |
| Colaborator | Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de colaborare semnat intre persoana si CertDigital sau intre CertDigital si compania pentru care lucreaza persoana respectiva |
| Compromitere | O incalcare a unei politici de securitate care duce la pierderea controlului asupra unei informatii cu caracter sensibil |
| Confidentialitate | Reprezinta un principiu de securitate care restrange accesul datelor doar la persoanele autorizate. |
| Control al accesului | Limitarea si verificarea accesului la sistemele informatice cu scopul de a elimina utilizarea |

| | |
|---|---|
| | neautorizata a acestora |
| Criptare | Transformarea textului clar in text criptat cu scopul de a ascunde continutul informatiilor pentru a preveni modificarea si utilizarea neautorizata a acestora. |
| Date in forma electronica | Reprezentari ale informatiei intr-o forma conventionala adecvata crearii, prelucrarii, trimiterii, primirii sau stocarii acesteia prin mijloace electronice |
| Declaratia Praticilor de Certificare | Document ce reglementeaza activitatea de furnizare a serviciilor de certificare |
| Dispozitiv de creare a semnaturii electronice | Sisteme software si/sau hardware configurate, utilizate pentru a implementa datele de creare a semnaturii electronice |
| Entitate | Termen folosit pentru a descrie un client. De exemplu, o entitate poate fi o companie, un trust, sau o persoana fizica |
| Evaluare de conformitate | Revizuire periodica efectuata asupra anumitor procese, in urma careia se stabileste gradul de conformitate cu standardele cerute |
| Extensii | Campuri de extensie in certificatele X.509 v.3 |
| Firewall | Reprezinta un echipament sau o serie de echipamente configurate astfel incat sa asigure filtrarea, criptarea sau intermedierea traficului intre domenii diferite de securitate pe baza unor reguli predefinite |
| Furnizor de servicii de certificare | Autoritate de incredere ce furnizeaza servicii de creare, semnare si emitere de certificate |
| Generator de chei | Echipament criptografic folosit pentru generarea de chei criptografice |
| Hash-code | Funcţie care returneaza amprenta unui document electronic |
| HTTPS | Protocol de comunicare client-server similar HTTP, care permite vizualizarea de pagini web intr-un mod |

| | |
|---|---|
| | securizat bazat pe criptarea informaţiilor transmise de catre server şi decriptarea acesteia de catre client, folosind certificatul serverului, acceptat la iniţializarea conexiunii. |
| Incident de Securitate a Informatiei | Eveniment declansat accidental sau intentionat care altereaza informatiile si/sau echipamentele si care provoaca pierderea partiala sau completa a confidentialitatii/ integritatii informatiilor ori indisponibilitatea acestora. |
| Integritate | Principiu de securitate care asigura ca informatiile si sistemele informationale nu sunt modificate in mod accidental sau in mod voit. |
| Internet | Reprezinta o multitudine de calculatoare conectate intr-o retea globala care permite partajarea datelor (din institutii academice, institute de cercetare, companii private, agentii guvernamentale, indivizi, etc.) care pot fi accesate de la distanta |
| Lista Certificatelor Revocate | Document emis la anumite intervale de timp in care se specifica certificatele care au fost revocate sau suspendate inainte de expirarea perioadei de valabilitate. Informatiile specificate in aceasta lista includ numele emitentului, data publicarii, data urmatoarei actualizari, numerele de serie ale certificatelor revocate sau suspendate si motivele pentru care au fost revocate sau suspendate. |
| Modul de securitate hardware | Echipament hardware controlat printr-un software, care realizeaza operatii criptografice (inclusiv criptare si decriptare) |
| Nume distinct (ND) | Grup de informatii ale unei entitati ce alcatuiesc un nume distinctiv prin care se deosebeste de alte entitati similiare |
| Organism de | Ministerul Comunicatiilor si Societatii Informationale in |

| | |
|---|---|
| supraveghere | calitate de autoritate de reglementare si supraveghere specializata in domeniu |
| Organism de evaluare a conformitatii | Organism acreditat conform cu prevederile Regulamentului (UE) nr. 910/2014 ca fiind competent sa efectueze evaluarea conformitatii unui prestator de servicii de incredere calificat si a serviciilor de incredere calificate pe care acesta le presteaza |
| Pagina web | Document electronic, disponibil prin Internet |
| Pereche de chei | Pereche complementara de chei de criptare generate de Autoritatea de Certificare si formatate intr-o cheie privata şi o cheie publica. Cheia publica este distribuita intr-un certificat eliberat de catre Autoritatea de Certificare |
| Pereche de chei asimetrice | Pereche de chei in relatie unde cheia privata defineste transformarea privata si cheia publica defineste transformarea publica. |
| Parola | Sir de caractere unic asociat unui utilizator cu scopul de a valida identitatea acestuia. |
| Perioada de valabilitate | Perioada cuprinsa intre data intrarii in vigoare a certificatului si data de expirare a valabilitatii sau data la care este revocat |
| Persoana de incredere | Angajat permanent sau temporar al organizatiei ce detine drepturi de administrare a infrastructurii de incredere din cadrul organizatiei |
| Prestator de servicii de incredere | Persoana fizica sau juridica care presteaza unul sau mai multe servicii de incredere ca prestator de servicii de incredere calificat sau necalificat |
| Prestator de servicii de incredere calificat | Prestator de servicii de incredere care presteaza unul sau mai multe servicii de incredere calificate si caruia i se acorda statutul de calificat de catre organismul de supraveghere |

| | |
|---|---|
| PKI | Infrastructura de chei publice |
| PKCS (Public-Key Cryptography Standards) | Standard de criptografie a cheilor publice |
| PKCS#10 | Sintaxa standard pentru cererile de certificat si standard de criptare a cheii publice #10, dezvoltat de catre RSA Security Inc. |
| Politica de Securitate a Informatiei | Politica ce sta la baza modului de abordare, de catre CertDigital, a problemelor referitoare la Managementul Securitatii Informatiilor. |
| Securitatea Informatiilor | Pastrarea confidentialitatii, integritatii si disponibilitatii informatiilor si asigurarea autenticitatii, responsabilitatii, nonrepudierii si acuratetii informatiei in scopul asigurarii continuitatii afacerii, minimizarii riscurilor si maximizarii profitului operational si a oportunitatilor de afaceri. |
| Semnatar | Persoana specificata ca subiect al certificatului ce detine cheia privata aferenta cheii publice din certificat. |
| Semnatura electronica | Date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna |
| SHA256 | Algoritm securizat de hash-code |
| Sigiliu electronic | Date in format electronic atasate la sau asociate logic cu alte date in format electronic pentru asigurarea originii si integritatii acestora din urma |
| Sistem de Detectie A Intruziunilor (IDS) | Sistem folosit pentru detectarea accesului neaprobat intr-o retea sau o statie de lucru. |
| DC1 si DC2 | Centru de date principal si centrul de date secundar (de backup) |
| Sistem de semnatura asimetrica | Sistem bazat pe tehnici asimetrice in care transformarea privata este folosita pentru semnare si transformarea publica este folosita pentru verificare. |

| | |
|---|---|
| SSL | Canal de comunicatie privat intre un server WEB si browser-ul client |
| Utilizator | Beneficiarul serviciilor de certificare, care, in baza unui contract incheiat cu un furnizor de servicii de certificare, denumit in continuare furnizor, deţine o pereche funcţionala cheie publica-cheie privata şi are o identitate probata printr-un certificat digital emis de acel furnizor |

# 1. Introducere

## 1.1. Marca CertDigital

CertDigital reprezinta marca inregistrata sub egida caruia S.C. Centrul de Calcul S.A. furnizeaza serviciile de certificare si marcare temporala. De fiecare data cand in continutul acestui document se fac referiri la CertDigital, acele referiri implica compania Centrul de Calcul S.A.

## 1.2. Continut

Declaratia Practicilor de Certificare defineste procedurile de lucru implementate de CertDigital in procesul de furnizare a serviciilor de certificare, respectiv de emitere si administrare a certificatelor digitale in conformitate cu prevederile legislative aplicabile nationale precum si cele ale Regulamentului (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna.

Prin natura serviciilor prestate, CertDigital asigura confidentialitatea prelucrarii datelor personale ale clientilor printr-o declaratie de confidentialitate agreata de catre parti.

Acest document include printre practicile si procedurile de lucru definite aspecte precum:

- Obligatiile si responsabilitatile autoritatii de certificare si inregistrare, respectiv ale utilizatorilor certificatelor digitale;
- Aspectele juridice privind furnizarea serviciilor de certificare de catre CertDigital;
- Mecanismele implementate pentru confirmarea identitatii entitatilor care au aplicat pentru obtinerea unui certificat;
- Descrierea procedurilor operationale privind emiterea si administrarea certificatelor;
- Procesele de auditare si revizuire a politicilor de securitate din cadrul CertDigital;

- Controalele de acces fizic, de securitate a informatiei, de personal si de management al cheilor implementate de catre CertDigital;
- Lista de certificate emise, precum si lista certificatelor revocate de catre CertDigital;
- Modalitatea de administrare practicilor de certificare CertDigital.

## 1.3. Audienta si aplicabilitate

CertDigital furnizeaza servicii de incredere calificate, certificate (simple si/sau calificate), marci temporale si sigilii electronice pentru orice tip de utilizator, in limita legilor in vigoare.

In sfera de aplicabilitate a prezentului document se include totalitatea participantilor la serviciile de certificare CertDigital, respectiv abonati, distribuitori sau alte parti contractante.

Prezentul document descrie procese referitoare la certificate calificate pentru aplicatii de securitate ridicata oferite utilizatorilor de servicii CertDigital ce permit tertilor, participanti in procesul de comunicare electronica verificarea semnaturilor digitale si a sigiliilor electronice. Validarea unei semnaturi digitale/ sigiliu electronic sau a unei tranzactii prin interactiunea cu certificatul digital CertDigital nu depinde de locul in care certificatul este emis sau de locul unde se utilizeaza semnatura digitala/sigiliul electronic si nici de distributia geografica a utilizatorului sau a autoritatii de certificare.

### 1.3.1. Autoritatea de certificare

Autoritatile de certificare reprezinta totalitatea entitatilor care emit certificate calificate sub aplicabilitatea unui set de practici si proceduri, care in functie de scopul ACP (autoritatea de certificare primara), poate fi acelaşi pentru fiecare ACP, sau poate diferi de la un ACP la altul. Autoritatile de certificare care emit certificate abonatilor-utilizatori finali sau altor autoritati de certificare, se subordoneaza ACP.

### 1.3.2. Autoritatea de inregistrare

Autoritatea de inregistrare este orice partener al CertDigital special mandatat de catre acesta pentru a realiza procesele de verificare si confirmare sau respingere a cererilor de inregistrare, emitere, reinnoire sau revocare a certificatelor digitale.

In cazul in care solicitantul trimite cerereea de inregistrare, emitere, reinnoire sau revocare a certificatelor digitale direct la sediul CertDigital sau prin sistemele informatice puse la dispozitie de catre acesta, Autoritatea de inregistrare va fi in acest caz chiar CertDigital.

Prin verificare, datele aferente cererilor sunt revizuite in scopul autentificarii solicitantului.

In situatia anularii unei cereri de inregistrare a unui abonat, respectiv de retragere a certificatului, Autoritatea de Inregistrare poate trimite cereri catre Autoritatea de Certificare corespunzatoare – pentru anularea cererii de inregistrare a unui utilizator si pentru retragerea certificatului acestuia.

### 1.3.3. Utilizatorii finali

Sfera utilizatorilor finali cuprinde atat abonatii, ca posesori de certificate digitale, dar si entitatile partenere care folosesc certificatele abonatilor in vederea autentificarii semnaturilor electronice ale acestora.

Certificatele digitale CertDigital sunt oferite pentru orice tip de utilizator in baza limitelor legislative aplicabile.

## 1.4. Reglementari aplicabile

Practicile si procedurile descrise in acest document in documentul prezent au fost dezvoltate in conformitate cu urmatoarele acte legislative:

- Regulamentul (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna;
- Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea;
- Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR;

- Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (inclusiv regulile privind comunicațiile electronice și cookie-urile)

## 1.5. Adresa de contact

Adresa: Str. Tudor Vladimirescu, nr. 17, Targu-Jiu, jud. Gorj

E-mail: office@certdigital.ro

Telefon: +40 253 214 767

Fax: +40 253 213 409

Alte informatii suplimentare despre practicile si procedurile de certificare CertDigital se pot obtine prin e-mail la adresa office@certdigital.ro.

## 1.6. Programul de funcționare

Programul de funcționare al sediului CertDigital este stabilit in intervalul 8:00 – 18:00 cu posibilitate de prelungire in situațiile in care acest lucru este necesar.

# 2. Prevederi generale

Capitolul de fata reglementeaza obligatiile si raspunderile atat din perspectiva autoritatilor de certificare si inregistrare cat si din perspectiva utilizatorilor prin prisma abonatilor si a entitatilor partenere.

Obligatiile si raspunderile stipulate in continuare sunt guvernate de acorduri mutuale stabilite intre parţile menţionate pe baza reglementarilor legislative in vigoare.

## 2.1. Obligatii

### 2.1.1. Obligatiile Autoritatii de Certificare

Printr-o politica de certificare asumata si pusa la dispozitia utilizatorilor, o autoritate de certificare isi atribuie o serie de obligatii fundamentale dupa cum urmeaza:

- Constituirea unui document (in speta, Declaratia Politicilor si Practicilor de Certificare) prin intermediul caruia sa se defineasca modalitatea de lucru, procedurile aplicabile, politica generala a CertDigital, obligatiile si drepturile partilor contractante etc. care sa fie aprobat de catre Conducere si publicat intr-un mediu accesibil utilizatorilor carora i se adreseaza;
- Desfasurarea activitatii in conformitate cu procedurile descrise in prezenta Declaratie;
- Implementarea unor resurse hardware si software fiabile care sa sustina buna desfasurare a activitatii in mod permanent in baza reglementarilor impuse de Autoritatile de Certificare, dar si din punct de vedere al afacerilor in mediul virtual;
- Procesarea cererilor de emitere de certificate doar printr-o Autoritate de Inregistrare cu care exista o asociere contractuala si care, de asemenea, isi desfasoara activitatea in maniera stabilita prin prezenta Declaratie;
- Asigurarea protecției datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri

de punere în aplicare a GDPR, precum și cu Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (inclusiv regulile privind comunicațiile electronice și cookie-urile).

- Informarea utilizatorilor asupra obligatiilor pe care le detin in baza acestui document, dar si asupra riscului la care se supun prin nerespectarea acestor obligatii;
- Revocarea certificatelor digitale, in cazul in care datele continute de certificat nu mai sunt de actualitate, in cazul compromiterii cheii private corespunzatoare certificatului sau in cazul in care utilizatorul certificatului a actionat contrar reglementarilor stipulate prin acest document. Aceasta situatie impune Autoritatii de Certificare obligativitatea anuntarii utilizatorului in cauza despre masurile luate;
- Asigurarea unei infrastructuri care sa permita folosirea serviciilor de inregistrare, emitere si intrare in posesie a certificatelor exclusiv prin mijloace electronice;
- Crearea si administrarea permanenta a unui registru de evidenta a certificatelor emise de catre toate Autoritatile de Certificare Primara subordonate care sa permita la orice moment accesul la informatii privind certificatele emise.

### 2.1.2. Obligatiile Autoritatii de Inregistrare

Autoritatea de Inregistrare isi defineste activitatea in jurul proceselor de validare, aprobare sau respingere a cererilor pentru certificat prin cererea revocarii certificatelor şi prin aprobarea cererilor de reinnoire.

Autoritatea de Inregistrare este responsabila pentru informatia colectata, motiv pentru care, cerinţele de securitate impuse autoritatilor de certificare sunt asemanatoare celor impuse oricarei autoritati de intregistrare.

Printre obligatiile Autoritatii de Inregistrare se numara:

- Implementarea unor resurse hardware si software fiabile care sa sustina buna desfasurare a activitatii in mod permanent;

- Desfasurarea activitatii in conformitate cu procedurile descrise in prezenta Declaratie;
- Asigurarea protecției datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, precum și cu Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (inclusiv regulile privind comunicațiile electronice și cookie-urile).
- Asigurarea corectitudinii datelor de utilizator ce sunt validate si trimise catre Autoritatea de Certificare pentru a fi incluse in certificat;
- Furnizarea catre clienti a contractelor ce trebuie semnate, pentru a intra in posesia unui certificat;
- Folosirea cheilor private ale operatorilor doar in scopurile prezentate in aceasta Declaratie;
- Livrare cheilor si/sau a certificatelor catre abonati;
- Protectia codului PIN si a cheii private ce urmeaza a fi livrate unui abonat fata de posibilele interceptari.

### 2.1.3. Obligatiile utilizatorului

Documentul de fata reprezinta parte integranta in contractul dintre Furnizorul de Servicii de Certificare si utilizatorul certificatului. Astfel, pe baza acestui contract, utilizatorul isi exprima acordul integrarii sale in sistemul de certificare in concordanta cu normele specificate prin acest document si se supune urmatoarelor obligatii:

- Subscrierea la termenii contractuali;
- Supunerea la regulile si procedurile descrise in prezenta Declaratie;
- Cunoasterea informatiilor generale referitoare la certificate, semnaturi electronice si PKI.
- Obtinerea certificatelor de chei publice din partea autoritatilor de certificare si inregistrare;

- Furnizarea de date valide catre autoritatile de certificare si inregistrare. Utilizatorii sunt obligati sa ia la cunostinta consecintele ce pot aparea ca urmare a folosirii unor date falsificate;
- Acceptarea semnaturii electronice create prin intermediul unei chei private si asociata unui certificat aprobat care contine cheie publica ca semnatura proprie si recunoasterea faptului ca certificatul nu a fost invalid (in afara datei de valabilitate), revocat sau suspendat la crearea semnaturii;
- Aprobarea certificatului care i-a fost emis. Prin aceasta aprobare se lanseaza in aplicare catre utilizator garantiile si obligatiie CertDigital in legatura cu un anumit tip de certificat;
- Utilizarea certificatelor de chei publice si chei private corespunzatoare numai in scopurile definite prin certificat si in concordanta cu ariile de aplicabilitate si restrictiile stabilite prin Declaratia practicilor de certificare.
- Adoptarea masurilor necesare pentru stocarea in conditii de siguranta a cheii private din cadrul unei perechi de chei;
- Notificarea emitentului de certificat a situatiilor cand constata incalcarea securitatii cheilor private sau are suspiciuni asupra acesui fapt;

## 2.2. Raspunderi

### 2.2.1. Raspunderea Autoritatii de Certificare

**CertDigital**, în calitate de prestator calificat de servicii de încredere (QTSP), își asumă răspunderea conform Regulamentului (UE) nr. 910/2014 (eIDAS) și Legii nr. 214/2024, actul național care aplică eIDAS. Răspunderea QTSP pentru prejudiciile cauzate prin nerespectarea obligațiilor prevăzute de eIDAS este reglementată de art. 13.

CertDigital este răspunzător față de orice persoană fizică sau juridică pentru prejudiciile cauzate intenționat sau din neglijență prin nerespectarea obligațiilor prevăzute de eIDAS pentru serviciile sale calificate. Pentru QTSP, neglijența se presupune, cu posibilitatea de a dovedi că prejudiciul s-a produs fără intenția sau culpa sa.

În special, pentru certificatele calificate, CertDigital răspunde:

- pentru exactitatea informațiilor din certificat la momentul emiterii;
- pentru legătura dintre datele de verificare a semnăturii din certificat și titularul identificat (inclusiv faptul că titularul deține datele de generare a semnăturii la momentul emiterii, după caz);
- pentru gestionarea stării certificatului (inclusiv suspendarea/revocarea) conform legislației și politicilor publicate, astfel încât terții să poată verifica în mod rezonabil validitatea la momentul utilizării;
- pentru respectarea cerințelor din eIDAS/Legea 214/2024 și din politicile/declarațiile de practici (CP/CPS/PS).

Înainte de emitere, CertDigital desfășoară verificări conforme eIDAS și Legii 214/2024 și politicilor sale (CP/CPS), incluzând cel puțin:

- identificarea solicitantului prin proceduri adecvate tipului de certificat;
- confirmarea deținerii cheii private corespunzătoare cheii publice din certificat (sau controlul asupra acesteia, în cazul soluțiilor gestionate/QSCD);
- verificarea exactității informațiilor ce vor fi înscrise în certificat.

CertDigital poate înscrie în certificate restricții de utilizare și/sau limite valorice ale operațiunilor. QTSP nu răspunde pentru utilizarea certificatului cu încălcarea acestor restricții sau peste limite, în măsura în care restricțiile/limitele sunt publice și inteligibile terților.

CertDigital dispune de mijloace financiare adecvate și de o poliță de asigurare de răspundere menținută conform cerințelor autorității de supraveghere și procedurii de acordare/suspendare/retragere a statutului de QTSP. Sumele și condițiile de acoperire sunt aliniate la cadrul legal aplicabil QTSP.

CertDigital asigură securitatea, fiabilitatea și continuitatea serviciilor prin măsuri tehnice și organizatorice conforme cu eIDAS și cu standardele ETSI/ISO relevante (de ex. ETSI EN 319 401 pentru cerințe generale TSP, precum și standardele de securitate și operare), respectiv ISO/IEC 27001/27002 pentru managementul securității informației. Practicile operaționale se aliniază cadrelor COBIT/ITIL, acolo unde este relevant, pentru procese și guvernanță.

CertDigital operează cu personal cu experiență în securitate informațională și servicii de încredere; rolurile critice respectă segregarea atribuțiilor și principiul „four-eyes”.

Din punct de vedere al resurselor umane folosite, CertDigital dispune de personal cu experienta in domeniul securitatii informatice si al semnaturii electronice.

Personalul este verificat, instruit și auditat periodic, conform politicilor interne, eIDAS/Legea 214/2024 și standardelor ETSI/ISO aplicabile.

### 2.2.2. Raspunderea Autoritatii de Inregistrare

Autoritatea de Inregistrare detine raspunderea strict pentru aspectele ce fac referire la obiectul activitatii sale.

Relatia dintre utilizator si autoritatile de emitere a certificatelor cu referire la garantiile si limitele responsabilitatii intre parti se supune si este gurvernata pe baza acordurilor agreate si a normelor legislative aplicabile.

### 2.2.3. Raspunderea utilizatorilor

Aspectele mentionate in capitolul 2.1.3 privind obligatiile si garantiile utilizatorilor constituie baza de raspundere juridica a utilizatorilor. Contractul de furnizare a certificatului digital incheiat intre client si CertDigital include conditiile in care aceasta raspundere intervine.

Furnizorul de servicii de certificare CertDigital va pretinde clientilor despagubiri in situatiile de incalcare a prevederilor prezentei Declaratii dupa cum urmeaza:

- Furnizarea unor informatii false pentru emiterea certificatului;
- Folosirea unui nume care contravine semnificativ drepturilor de proprietate intelectuala a unui tert;
- Neglijarea masurilor de securitate asupra cheii private avand ca efect pierderea, compromiterea sau folosirea neautorizata a cheii private;

## 2.3. Interpretare si aplicare

### 2.3.1. Legea aplicabila

Prevederile si activitatile desfasurate in baza prezentului document vor respecta dispozitiile prevazute de normele legislative nationale si internationale, in domeniul serviciilor de certificare.

Reglementarile pentru furnizarea de servicii de certificare pentru certificate calificate sunt in particular definite Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea, respectiv in Regulamentul (UE) nr. 910/2014 privind identificarea electronica si serviciile de încredere pentru tranzactiile electronice pe piata interna.

### 2.3.2. Intrarea in vigoare

Intrarea in vigoarea a Declaratiei Practicilor si Politicilor de Certificare se realizeaza la data notificarii catre Organismul de Supraveghere si este valabil pana la data emiterii unei noi versiuni.

### 2.3.3. Aplicabilitate

Normele specificate in prezenta Declaratie sunt aplicabile autoritatilor de emitere a certificatelor pe seama obligatiilor mentionate in capitolul 2.1 si utilizatorilor in momentul in care incheie un contract in conformitate cu prevederile acestui document.

## 2.4. Onorarii

### 2.4.1. Onorarii pentru emiterea sau prelungirea a unui certificat

Serviciile CertDigital sunt oferite contracost, iar tarifele exacte sunt stabilite in functie de natura si complexitatea serviciilor oferite.

### 2.4.2. Onorarii pentru servicii conexe

CertDigital isi rezerva dreptul de a percepe tarife suplimentare aferent serviciile prestate(ex. servicii de implementare, consultanta, instruire, etc.) daca acestea fac obiectul acordului dintre parti.

## 2.5. Publicarea si depozitarea informatiilor

### 2.5.1. Publicarea informatiilor de catre CertDigital

Pentru publicarea informatiilor de interes public, CertDigital implementeaza o interfata dedicata accesibila la adresa www.certdigital.ro prin care se inglobeaza urmatoarele tipuri de informatii:

- Declaratia Practicilor de Certificare CertDigital (varianta in vigoare si varianta anterioara);
- Declaratia de confidentialitate privind procesarea si stocarea informatiilor personale;
- Rapoarte de audit;
- Certificate emise;
- Lista certificatelor revocate.

### 2.5.2. Frecventa publicarilor

Publicarea actualizarilor aferente informatiilor de mai sus se realizeaza dupa cum urmeaza:

- Declaratia Practicilor de Certificare – este publicata in conformitate cu prevederile Capitolului 7 („Administrarea documentului”);
- Rapoartele de audit – odata cu furnizarea lor de catre auditor;
- Certificatele emise – sunt publicate imediat dupa emitere;
- Lista certificatelor revocate – este publicata dupa fiecare revocare a unui certificat intr-un interval de maxim o zi.

### 2.5.3. Accesul la informatiile publicate

Toate informatiile publicate de CertDigital prin interfata online au caracter public si nu se solicita drepturi speciale pentru vizualizare.

Pentru prevenirea accesului neautorizat la depozitul de stocare a informatiilor, CertDigital a impelementat o serie de masuri logice si fizice care asigura protectie impotriva adaugarii, modificarii sau stergerii informatiilor publicate.

## 2.6. Evaluarea conformitatii

In concordanta cu prevederile art. 20, alin. (1) din Regulamentul (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna, CertDigital contracteaza o data la 24 de luni un organism de evaluare a conformitatii acreditat cu scopul de a confirma ca CertDigital, in calitate de prestator de servicii de incredere calificat si serviciile de incredere pe care le presteaza indeplinesc cerintele prevazute in Regulamentul (UE) nr. 910/2014

Ca parte a acestor evaluari, CertDigital urmareste obtinerea unor revizuiri suplimentare privind administrarea riscului si consolidarea unui nivel maxim de securitate si conformitate cu politicile si practicile documentate.

## 2.7. Confidentialitatea

Informațiile aflate în posesia CertDigital sunt colectate, păstrate și prelucrate în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR, cu Legea nr. 506/2004 (actualizată) privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, precum și cu Regulamentul (UE) nr. 910/2014 (eIDAS) și Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere.

Accesul la certificatele calificate poate fi obtinut doar daca detinatorul certificatului a fost de acord cu publicarea certificatului.

Utilizarea si prelucrarea datelor persoanale de catre CertDigital se realizeaza strict in masura in care aceasta activitatea este necesara emiterii unui certificat calificat.

CertDigital asigura toate masurile de protectie impotriva accesului neautorizat asupra datelor personale si a celor legate de organizatie care nu sunt incluse in certificat, inclusiv in cursul procesului de generare a datelor de creare a semnaturilor.

## 2.8. Drepturile de proprietate intelectuala

Prezenta Declaratie reprezinta proprietatea intelectuala a CertDigital.

CertDigital detine toate drepturile de proprietate intelectuala asupra certificatelor calificate emise de aceasta, iar reproducerea certificatelor este permisa exclusiv cu acordul CertDigital.

Perechile de chei corespunzatoare certificatelor Autoritatii de Certificare calificate CertDigital reprezinta proprietatea CertDigital.

Perechile de chei corespunzatoare certificatelor semnatarilor sunt proprietatea semnatarilor specificati in aceste certificate.

# 3. Proceduri de administrare a certificatelor

Obţinerea unui certificat digital calificat se face in mai multe etape, fiecare etapa având un rol bine determinat şi desfaşurându-se sub responsabilitatea solicitantului, al Autoritaţii de Inregistrare sau al Autoritaţii de Certificare.

## 3.1. Cererea unui certificat

In situatia in care o entitate doreste obtinerea unui certificat digital, trebuie sa inainteze o solicitare catre CertDigital respectand procedura descrisa in prezenta Declaratie. Aceste solicitari sunt procesate de catre Autoritatea de Certificare CertDigital si in functie de caz sunt aprobate sau nu.

Generarea cheilor se desfasoara intr-un mediu securizat si se poate realiza de catre Autoritatea de Certificare, Autoritatea de Inregistrare sau de catre semnatar. Pentru generarea cheilor se utilizeaza dispozitive securizate si aprobate spre a fi utilizate in scopul crearii a semnaturilor electronice. Functionalitatea acestor dispozitive nu include exportarea cheilor private generate.

Aferent obtinerii unui ceritificat, clientul va semna documentul „Acord utilizator” prin intermediul caruia isi exprima acordul de prelucrare a datelor cu caracter personal, ia la cunostinta despre obligatiile ce ii revin, in calitate de titular al unui certificat calificat si totodata isi asuma responsabilitatea privind veridicitatea informatiilor furnizate. Tot prin intermediul acestui document, clientul isi exprima acordul cu privire la publicarea certificatului emis in Registrul Public CertDigital al certificatelor emise.

Procesul de inregistrare a unui client se realizeaza in baza unor politici si proceduri prin care Autoritatea de Certificare obtine toate datele necesare identificarii unei entitati inainte de a-i emite un certificat calificat.

Autoritatea de inregistrare are obligaţia de a verifica si a face copii dupa toate documentele originale prezentate de catre client, copii pe care le va pastra in conformitate cu normele de arhivare a informaţiilor cu caracter personal.

In cadrul procesului de eliberare a unui certificat digital calificat se executa urmatorii pasi:

- **Pasul 1**: Identificarea persoanei, exclusiv pe baza actului de identitate prezentat:

- Validarea actului de identitate in vederea stabilirii corespondentei cu modelul de Carte de Identitate Românească (sa fie o carte de identitate românească).
- Verificarea pozei din actul de identitate in vederea corespondentei cu persoana fizica prezenta.
- Verificarea valabilității actului de identitate .
- Verificare integrității fizice a actului de identitate.
- Scanarea și validarea MRZ folosind aplicatia RA Client
- Daca aplicatia RA Client valideaza actul de identitate se trece la completarea cererii in platforma web.

- **Pasul 2**: Se genereaza o cerere de emitere certificat prin intermediul platformei web:
- Se introduce CNP-ul clientului, sau pentru persoanele care nu sunt cetaţeni români, se introduce codul unic de identificare similar. Sistemul valideaza CNP-ul romanesc conform algoritmului pentru suma de control.
- Se completeaza adresa de e-mail si datele personale (nume, prenume, adresa, serie şi numar act de identitate, alte informaţii de contact, etc ).
- Se introduc informaţiile optionale ce se doresc a fi inscrise in certificat: instituţia, departamentul sau funcţia .
- Se fotocopiaza si se ataseaza copiile documentelor in original prezentate de client
- Se trimite cererea spre aprobare.

Operatorii din cadrul Departamentului validare si emitere servicii electronice calificate procedează la validarea si aprobarea cererii de emitere a certificatului, astfel:

- Validarea actului de identitate in vederea stabilirii corespondentei cu modelul de Carte de Identitate Românească (sa fie o carte de identitate românească).
- Verificarea valabilității actului de identitate

- Verifica informațiile înscrise in cerere prin identificarea documentelor asociate in care se regăsește fiecare informație in parte. Orice informație înscrisa in certificat trebuie sa se regăsească intr-un document atașat la cerere, in caz contrar, cererea este data in corectare sau refuzata, după caz.
- Detalierea procesului de validare a unei cereri se regaseste in documentul intern Anexa - Regulament privind identificarea și cererea certificatelor digital calificate.

Dacă toate informatiile au fost validate cu succes, cererea este marcata ca aprobata si este trecuta pe fluxul de emitere a unui certificat digital calificat.

Documentele necesare pentru emiterea unui certificat sunt:

| | | |
|---|---|---|
| Act identitate | **OBLIGATORIU** | Se accepta documente de identitate si pașapoarte conform secțiunilor „A – Passport" si „B – Identity card" specifice fiecărei tari in parte din registrul de documente publicat la https://www.consilium.europa.eu/prado/en/search-by-document-country.html |
| Acord Utilizator | **OBLIGATORIU** | Formatul listat din portal |
| Contract | **OBLIGATORIU** | Listat din portal si semnat. Contractul se generează anterior eliberarii certificatului. Se accepta si SEMNAREA ELECTRONICA a contractului, cu certificatul digital calificat, aflat in perioada de valabilitate, emis anterior generarii cererii de emitere a noului certificat. |
| | | |
| **Opționale** | **Se solicita DOAR când** | |
| | | |
| CUI | Se dorește înscriere în certificat a cel puțin una din informatiile: **organizația**, **titlu**, **funcția** sau se emite un **sigiliu calificat.** | |
| Constatator | Solicitantul este **administratorul** societății si dorește in certificat cel puțin una din : **organizația**, **titlu**, **funcția.** | |
| Împuternicire | Solicitantul este **angajat** al societății si dorește in certificat cel puțin una din informatiile: **organizația**, **titlu**, **funcția** | |
| Adeverința/Certificat DSP/CASA cod parafa | Solicitantul este medic si dorește înscrierea codului de parafă în certificat | |

| | |
|---|---|
| Documente justificative | Pentru orice alte informatii ce urmeaza a fi inscrise in certificat. |

### 3.1.1. Tipuri de nume

Fiecare entitate trebuie sa isi defineasca un Nume Distinct in campul subiect al certificatului in concordanta cu standardul X509 V3.

### 3.1.2. Folosirea pseudonimelor

In conformitate cu Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea, certificatele CertDigital permit folosirea unor pseudonime ca alternativa a numelui prin completarea unui camp suplimentar in formularul de inregistrare.

### 3.1.3. Necesitatea utilizarii unui nume cu inteles

Numele corespunzator Subiectului din certificat trebuie sa reprezinte utilizatorul certificatului intr-o maniera simpla de inteles si trebuie sa aiba o asociere rezonabila cu numele real al utilizatorului autentificat.

### 3.1.4. Unicitatea numelor

Numele Distinct trebuie sa fie unic pentru fiecare subiect certificat de catre Autoritatea de Certificare CertDigital. Daca numele prezentat de catre abonat nu este unic sunt anexate la denumirea comuna numere si litere suplimentare pentru a asigura unicitatea

Utilizatorii nu pot instraina certificatele care le-au fost acordate.

### 3.1.5. Procedura de rezolvare a litigiilor aparute din folosirea numelui

Solicitantilor de certificate CertDigital le este interzisa folosirea unor nume prin care se incalca drepturile de proprietate intelectuala. CertDigital nu verifica daca un solicitant de certificat detine drepturi de proprietate intelectuala pentru numele inscris pe cerere si nu este responsabil pentru solutionarea disputelor aparute din aceasta cauza.

CertDigital este indreptatita sa respinga sau sa suspende cererea unui abonat in cadrul conflictelor aparute fara a-si asuma vreo responsabilitate in acest sens.

## 3.2. Emiterea unui certificat

Informatiile furnizate de solicitant prin cererea de emitere a certificatului sunt procesate de catre CertDigital in concordanta cu prevederile prezentului document.

Aceasta procesare se realizeaza de catre un responsabil cu validarea solicitarilor de certificate. Validarea sau refuzul cererii de emitere a certificatului calificat se realizeaza folosind aceeaşi aplicaţie web, descrisa in cadrul etapei de inregistrare, numai ca acest responsabil are un cont special, care ii ofera drepturi sporite faţa de un client obişnuit.

De asemenea, in cadrul acestei etape se verifica plata serviciilor de certificare, pe care solicitantul trebuie sa o faca utilizând orice metoda de plata acceptata legal.

In cazul in care rezultatele aferente acestor procesari indeplinesc in mod valid conditiile de autentificare CertDigital aproba cererea pentru certificate, respectiv o respinge daca sunt identificate neconformitati.

Daca cererea a fost validata, sistemul va trimite un e-mail catre solicitant, care va conţine un URL catre o pagina de unde se va putea descarca certificatul emis.

## 3.3. Perioada de valabilitate si formatul certificatului

Perioada de valabilitate a certificatelor calificate emise de CertDigital este de unu, doi sau trei ani de la data emiterii in conformitate cu Legea 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale si prestarea serviciilor de încredere bazate pe acestea, si cu Regulamentul (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna, iar formatul respecta standardul X509 V.3.

## 3.4. Registrul electronic de evidenta a certificatelor emise

CertDigital mentine in permanenta un Registru electronic in care sunt evidentiate certificatele emise si in care se pot vedea informatiile referitoare la certificate:

- data si ora exacta la care certificatul a fost eliberat;

- data si ora exacta la care expira certificatul;
- daca este cazul, data si ora exacta la care certificatul a fost suspendat sau revocat, inclusiv cauzele care au condus la suspendare sau la revocare.

Registrul electronic de evidenta a certificatelor eliberate este disponibil permanent pentru consultare prin Internet prin website-ul CertDigital.

## 3.5. Acceptarea certificatului

CertDigital va trimite confirmarea de emitere a certificatului catre utilizatori impreuna cu procedurile de intrare in posesie.

Descarcarea certificatului calificat se realizeaza de catre solicitantul certificatului si este nevoie ca Dispozitivul securizat de creare a semnaturii electronice sa fie conectat la calculatorul de la care se efectueaza aceste acţiuni.

Desfasurarea acestei activitati se realizeaza prin intermediul unei conexiuni Internet si presupune folosirea in mod obligatoriu a unei conexiuni securizate pe protocolul HTTPS impusa de serverul CertDigital.

Utilizatorii sunt obligati sa verifice continutul certificatului la primirea acestuia, in speta corectitudinea datelor si complementaritatea cheii publice cu cea privata pe care o detine si sa notifice catre CertDigital orice eroare aparuta in acest sens. In astfel de situatii, CertDigital se obliga sa anuleze certificatul emis si sa asigure re-emiterea unui nou certificat.

Dupa o perioada de 7 zile calendaristice de la primire, certificatele emise sunt considerate validate de catre utilizatori.

Pe baza acordului agreat de utilizator la momentul solicitarii certificatului, CertDigital va publica oricare certificat nou emis in depozitul de informatii.

Odata cu acceptarea certificatului, utilizatorul accepta reglementarile prezentei Declaratii si se supune utilizarii certificatului in conformitate cu conditiile impuse.

Autoritatea de Inregistrare stocheaza copiile documentelor si declaratiilor prezentate de clienţi la emiterea certificatelor. De asemenea, Autoritatea de Inregistrarea, pastreaza variantele printate ale certificatelor calificate emise.

Certificatele emise existente in baza de date pot fi vizualizate folosind funcţia de cautare a aplicaţiei de certificare.

## 3.6. Revocarea unui certificat

Utilizatorul unui certificat poate revoca capacitatile functionale ale certificatului in cazul compromiterii cheii private intr-o forma iremediabila sau in cazul in care informaţiile din certificat nu mai corespund realitaţii.

Procesul de revocare poate fi cerut de catre utilizator sau de catre un responsabil care are drepturi de revocare a certificatelor, daca Autoritatea de Certificare CertDigital considera ca este necesara revocarea certificatului, conform legislatiei in vigoare.

Pe baza parolei pe care a introdus-o in procesul de emitere a certificatului calificat, un utilizator poate accesa in mediu online o adresa specifica la care poate revoca certificatul, introducând adresa de e-mail şi parola asociate acelui certificat.

In cazul in care utilizatorul a uitat parola, sau nu beneficiaza de servicii Internet, acesta va putea sa ceara Autoritaţii de Certificare sa revoce certificatul. Aceasta cerere va trebui sa fie insoţita şi de o legitimare a identitaţii utilizatorului, care va trebui sa faca dovada ca este posesorul certificatului ce se vrea revocat.

O revocare a certificatului poate sa aiba loc şi dupa o autosesizare a Autoritaţii de Certificare, sau la cererea anumitor autoritaţi ale statului conform legislatiei in vigoare.

Revocarea unui certificat nu intervine asupra tranzactiilor efectuate inainte de revocare si nici asupra obligatiilor care rezulta din respectarea practicilor descrise in acest document.

In momentul in care este revocat, certificatul este inclus in Lista Certificatelor Revocate din cadrul Registrului electronic de evidenta a certificatelor emise si este considerat invalid. Inregistrarea revocarii certificatelor se realizeaza imediat dupa inregistrarea cererii de revocare.

### 3.6.1. Circumstantele pentru revocare

Revocarea unui certificat se realizeaza in cazul in care:

- A fost emisa o cerere de revocare din partea semnatarului sau a unei entitati autorizate;

- Acordul dintre parti a expirat;
- CertDigital inceteaza furnizarea acestor servicii;
- Informatiile furnizate de semnatar in cererea de emitere sunt false;
- Cheia privata a utilizatorului este compromisa iremediabil;
- CertDigital decide ca eliberarea certificatului nu s-a realizat in conformitate cu procedurile solicitate prin Declaratia practicilor de certificare;
- CertDigital descopera faptul ca certificatul a fost eliberat unei alte persoane decat cea mentionata in certificat fara autorizarea acesteia;

### 3.6.2. Procedura pentru cererea de revocare

Cererea de revocare se poate depune dupa cum urmeaza:

- Semnatarul sau o entitate autorizata solicita revocarea unui certificat printr-un formular de revocare completat si semnat de mana la sediu Autoritatii de Certificare CertDigital.
- Semnatarul sau o entitate autorizata solicita revocarea unui certificat printr-o cerere de revocare in format electronic catre CertDigital. In acest caz, autentificarea revocarii se furnizeaza printr-o semnatura electronica calificata.
- Prin serviciile online puse la dispozitie de CertDigital.

### 3.6.3. Procedura pentru cererea de suspendare

CertDigital nu ofera posibilitatea suspendarii certificatelor emise.

## 3.7. Prelungirea perioadei de valabilitate pentru un certificat valid

Procesul de reinnoire a unui certificat si, implicit, de prelungire a perioadei de valabilitate presupune existenta unui certificat valid si a unei chei private corespunzatoare.

Prin reinnoire, CertDigital va emite un certificat cu aceeasi cheie publica ale carui informatii sunt preluate din certificatul anterior, dar cu modificarea numarului serial, a semnaturii emitentului si a perioadei de valabilitate.

## 3.8. Modificarea unui certificat valid

In cazul in care utilizatorul solicita emiterea unui nou certificat pe seama modificarii unor informatii din cel existent, CertDigital va emite in baza certificatului existent (daca acesta este valid) un nou certificat cu o noua cheie publica si un nou numar serial. Emiterea noului certificat se realizeaza dupa ce, in prealabil, au fost verificate si confirmate informatiile ce au suferit modificari.

# 4. Practici si proceduri operationale in domeniul IT

## 4.1. Procedura de control al accesului fizic

Regulile pe care se bazeaza masurile de control al accesului pornesc de la principiul ca toate drepturile sunt in general restrictionate in cazul in care nu exista o aprobare sau o autorizare explicita in conformitate cu politicile si procedurile CertDigital.

### 4.1.1. Amplasarea locatiei

Sediul principal al CertDigital este localizat in str. Tudor Vladimirescu, nr. 17, Targu-Jiu, judetul Gorj, Romania.

Sediul secundar al CertDigital este localizat in bulevardul Ecaterina Teodoroiu, nr. 354, Targu-Jiu, judetul Gorj, Romania.

### 4.1.2. Protectie impotriva accesului neautorizat

Sediul unde isi va desfasura activitatea Autoritatea de Certificare este dotat cu sistem de alarma si control acces (DVR stand-alone, camere de supraveghere, control acces, cititor de proximitate, senzori de miscare, senzori de inundatie, fum, alarme).

CertDigital are incheiat un contract cu firma specializata de securitate care asigura intervenţia unui echipaj in maxim 6 minute de la receptionarea semnalelor antiefractie, antiincendiu sau panica.

Camera unde se gasesc echipamentele Autoritaţii de Certificare este protejata suplimentar cu o uşa metalica antiefractie, accesul realizându-se pe baza unei cartele magnetice si a unui senzor de amprenta digitala, prin introducerea unui cod de securitate si actionarea unei chei, dispozitive pe care doar administratorul sistemului, ofiterul de securitate IT şi Directorul General le pot actiona.

### 4.1.3. Protectia cheilor private si a certificatelor calificate

Stocarea cheilor private utilizate la emiterea certificatelor se realizeaza prin echipamente securizate ce sunt atestate sa indeplineasca prevederile legislative

in vigoare si care nu pot fi falsificate. Pentru prevenirea oricarei tentative de acces neautorizat sau de falsificare a informatiilor sensibile, CertDigital implementeaza controale adecvate, revizuite periodic pentru a se asigura functionarea corespunzatoare.

Stocarea certificatelor calificate se realizeaza pe sisteme fiabile care permit posibilitatea introducerii si modificarii informatiilor din certificate numai persoanelor autorizate.

Consultarea certificatelor de catre terti se poate realiza doar în cazul in care există acordul titularului acestora;

De asemenea, sistemele CertDigital permit evidentierea oricarei modificari tehnice, care ar putea pune în pericol condiţiile de securitate implementate. Acest lucru este monitorizat permanent de catre persoanele autorizate din cadrul CertDigital.

### 4.1.4. Accesul fizic

Conducerea CertDigital indentifica drepturile de acces necesare angajatilor si comunica aceste drepturi personalului responsabil pentru a fi implementate in conformitate cu procedurile in vigoare.

Accesul in incinta sediului se face pe baza urmatoarelor reguli:

- Fiecare angajat CertDigital are implicit acces deplin la biroul sau;
- Pe toata durata de desfasurare a programului, fiecare angajat are acces in toate zonele, cu exceptia zonelor pe care managerul responsabil le-a marcat ca zone cu acces limitat;
- Dreptul de acces pentru colaboratori, consultanti, personal responsabil de curatenie etc. este permis numai in zonele in care isi desfasoara activitatea. Accesul se va face prin specificarea locului si a timpului necesar si va fi aprobat de catre managerul responsabil;
- Vizitatorilor le este permis accesul doar in spatiile de receptie, iar accesul in zonele securizate se va face numai in baza unei nevoi definite clar pentru desfasurarea activitatii si in permanenta supraveghere a unui angajat CertDigital;

- Personalul IT emite recomandari privind regulile de acces pentru consultantii si colaboratorii fiecarui departament care au o relatie de afaceri cu tertii.

### 4.1.5. Controale de mediu in zonele IT critice

Pentru stabilirea conditiilor optime in zonele IT critice au fost implementate urmatoarele masuri:

- Sisteme de aer conditionat si ventilatoare montate pe rack-uri care asigura o temperatura optima de functionare a echipamentelor IT;
- 2 echipamente UPS-uri fiecare având puterea de 6K. La aceste UPS-uri sunt conectate cele 6 servere, HSM-ul, router-ul, firewall-ul, switch-urile şi modem-urile de internet;
- Conexiune la o retea electrica separata pentru a asigura protectia impotriva supratensiunii;
- Pentru evitarea unor posibile amenintari (precum inundatiile), echipamentele din camera dedicata Autoritaţii de Certificare sunt aşezate intr-un rack inaltat, care este protejat printr-o incuietoare cu cheie.
- Sisteme de detectie a fumului si sisteme de stingere a incendiilor.

## 4.2. Politica de securitate

Masurile de securitate implementate de CertDigital care asigura desfasurarea activitatii de emitere certificate calificate in conditii optime se impart in:

- masuri de asigurare a redundantei pentru datele critice;
- masuri de asigurare a continuitatii serviciilor oferite;
- masuri de protectie fata de greselile personalului angajat;

### 4.2.1. Masuri de asigurare a redundantei pentru datele critice

**Sistem de mirroring pentru hard-disk-urile serverelor**

Siguranţa datelor este asigurata de sisteme ce se bazeaza pe matrici RAID Mirroring formate din doua discuri SATA de 6.0 TB - capacitate pentru fiecare server in parte. Duplicarea datelor asigura protecţie impotriva pierderii fizice a informaţiilor.

**Sistem de clustering pentru Autoritatea de Certificare**

Server-ul Autorităţii de Certificare (ca.certdigital.ro) este setat sa lucreze in clustering format din trei servere, asigurându-se astfel un nivel ridicat de disponibilitate a serviciilor.

**Proces de backup sistematic**

Datele de pe serverul ca.certdigital.ro, dar şi informaţiile de pe HSM sunt salvate şi arhivate periodic in conformitate cu prevederile procedurii de salvare si restaure a datelor.

### 4.2.2. Masuri de asigurare a continuitatii serviciilor oferite

In vederea asigurarii unei continuitati a serviciilor oferite, Autoritatea de Certificare dispune de conexiune la Internet prin doua linii oferite de furnizori diferiti, dupa cum urmeaza:

- RDS – linie principala fibra optica de 1000 Mbps garantat;
- ORANGE – linie back-up fibra optica de 1000 Mbps garantat.

### 4.2.3. Masuri de protectie fata de greselile personalului angajat

**Personal calificat in activitaţile de certificare**

Personalul angajat al Autorităţii de Certificare CertDigital este format din oameni calificaţi cu o bogata experienţa profesionala şi care poseda certificari şi diplome.

**Personal cu calificare si experienta**

Personalul care este nominalizat pentru a face parte din echipa care se ocupa cu activitatea de certificare trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.

**Segregarea activitaţilor**

Activitaţile sunt imparţite pe baza de roluri conform fişei de responsabilitaţi, astfel incât o activitate mai complexa sa poata fi dusa la capat numai cu acordul mai multor persoane. De exemplu, crearea de noi perechi de chei şi certificate pentru autoritaţile de certificare, unde administratorul sistemului şi responsabilul cu gestiunea autoritaţii de certificare trebuie sa colaboreze aşa cum este specificat in

cadrul procedurii operaţionale ce reglementeaza aceasta activitate. Mai mult decat atât, pentru activitaţi critice este necesar acordul scris al Directorului General.

Alt exemplu in acest sens este modalitatea de emitere a certificatelor calificate, unde exista responsabili cu introducerea datelor, responsabili cu validarea acestora, responsabili care pot revoca certificate, sau administratori care pot sa creeze noi conturi de utilizatori şi sa modifice rolurile acestora.

## 4.3. Procedura de salvare si restaurare a datelor

Programul de salvare a datelor este dezvoltat in baza unei evaluari a riscului efectuate de catre personalul IT din cadrul CertDigital.

Administratorul de sistem este responsabil de intregul proces de back-up si restaurare, care trebuie sa se desfaşoare conform curentei proceduri. Pentru procedura de restuarare este necesara, insa, o imputernicire scrisa, semnata de Conducerea CertDigital.

### 4.3.1. Procesul de salvare

La nivelul Autoritatii de Certificare sunt identificate doua seturi de date critice.

- baza de date MySQL Server si in fisiere, unde se pastreaza toate certificatele emise, şi informaţii despre acestea: beneficiarul, data emiterii, valabilitatea, etc.
- perechile de chei şi certificatele tuturor autoritaţilor din arborele de incredere CertDigital. Aceste informaţii stocate pe echipamentul Hardware Security Module (HSM).

Procesul de backup se realizeaza de catre administratorul de sistem, care include ambele puncte de la paragraful de mai sus.

Procesul de back-up al bazei de date MySQL Server se executa automat, programatic, folosind programe (scripturi de back-up) native MySQL Server si OS in urmatoarele etape:

- Full Back-up (Salvare Completa) – se executa automat zilnic o singura data la orele 23.00 si consta in salvarea in intregime a bazei de date: tabele, structura, proceduri stocate si functii, indecsi, rezultand o copie exacta a bazei de date la momentul salvarii si o salvare in intregime a certificatelor salvate in fisiere. Salvarea se efectueaza intr-un fisier denumit ca „backup_ *YYYYMMDD*hh:mm” , unde *YYYY.MM.DD* hh:mm reprezinta Anul.Luna.Ziua Ora:Minutul curent. Fisierul de backup generat este copiat in directorul „BKUP” destinat efecturii backup-urilor stocat pe diskul local.

- Salvarea datelor de pe HSM este efectuata pe SmarCard-urile producatorului, informatia este criptata si distribuita intr-o schema (M of N) care sa asigure redundanta. Smart-cardurile sunt tinute in siguranta intr-o locatie externa, autorizata pentru depozitarea valorilor .

- La nivelul Network Storage din DC1 sunt definite task-uri de replicare si sincronizare catre Network Storage din DC2 (sediul secundar, de backup) pentru fiecare dataset asociat masinilor virtuale din CertDigital. Aceste task-uri de sincronizare sunt executate la un interval de 15 minute.

### 4.3.2. Procedura de restaurare

Implementarea procedurilor de restaurare se desfasoara dupa cum urmeaza:

- Departamentul IT realizeaza cel putin trimestrial testarea mediului de back-up pentru a verifica faptul ca acesta poate fi folosit pentru restaurarea datelor.
- Testarea restaurarii – se realizeaza pe mediul de test si are ca scop verificarea functionarii corecte a datelor restaurate.

In cazul identificarii unor defecţiuni hardware (defectare a placii de baza, defectare a unitaţii de stocare sau altele) se trece la remedierea problemei prin inlocuirea componentelor defecte cu alte componente noi compatibile având caracteristicile tehnice identice cu cele ale componentelor iniţiale.

Dupa instalarea noilor componente in sistem, daca este necesar, se va trece la repopularea cu datele existente salvate inainte de apariţia problemei. Pentru executarea procedurii de restaurare a datelor de pe suportul de back-up (locatia de backup din Network Storage) este necesar acordul scris al Directorului General.

Procesul de restaurare se va realiza de catre administratorul de sistem sub supravegherea Directorului Tehnic, care va raspunde de acest proces.

## 4.4. Procedura de administrare a conturilor in sistemele CertDigital

Toate conturile de utilizator ale angajatilor CertDigital sunt identificate in mod unic printr-un nume de utilizator (care se va constitui pe baza numelui angajatului care foloseste contul) si o parola (care va fi stabilita pe baza regulilor si procedeelor mentionate in Procedura de Administrare a Parolelor).

Numele de utilizator al unui angajat se emite pe durata de desfasurare a activitatilor acestuia sub contract cu CertDigital si nu poate fi modificat decat in baza unor nevoi bine justificate (angajatul isi schimba in mod legal numele, in cadrul CertDigital isi desfasoara activitatea un alt angajat cu nume similar sau asemanator care poate crea confuzie etc.).

Aplicatiile informatice si de posta electronica din cadrul CertDigital permit definirea unor grupuri de utilizatori care specifica drepturile pe care utilizatorii care fac parte dintr-un grup le detin in utilizarea unui sistem informatic. Grupurile de utilizatori vor fi definite in conformitate cu responsabilitatile si necesitatile stricte pe care categoria de utilizatori careia i se asociaza le are.

Utilizatorii au obligatia de a-si folosi drepturile de acces in sistemele informatice care le-au fost acordate doar in vederea indeplinirii sarcinilor si responsabilitatilor alocate si se interzice folosirea informatiilor catre care au acces in alte scopuri decat cele precizate.

De asemenea, se interzice cu desavarsire angajatilor instrainarea sau “imprumutul” conturilor de acces proprii in reteaua de calculatoare, aplicatiile informatice sau sistemele de posta electronica catre alti angajati.

Contul unui utilizator poate avea mai multe stari, dupa cum urmeaza:

- *Activ* – contul este pe deplin operational;
- *Expirat* – parola corespunzatoare contului este expirata si pentru reactivarea sa este necesara generarea unei noi parole;
- *Dezactivat* – utilizarea contului de utilizator a fost oprita pe motivul incheierii contractului de munca intre angajatul posesor si Companie sau in cazul in care titularul de cont nu mai indeplineste criteriile de utilizare a contului.

### 4.4.1. Crearea conturilor de utilizatori

Definirea conturilor de utilizatori pentru reteaua de calculatoare, sistemele informatice sau sistemele de posta electronica din cadrul CertDigital se realizeaza de catre personalul de administrare a aplicatiilor din cadrul Departamentului IT.

La angajarea unei persoane noi in cadrul CertDigital care are nevoie de acces intr-unul sau mai multe dintre sistemele informatice, se va solicita de catre seful direct crearea conturilor de utilizator necesare prin completarea unui formular pentru crearea unui cont de utilizator. In cadrul formularului se vor detalia aplicatiile si sistemele pentru care se solicita contul de acces precum si drepturile si profilele de utilizator de care respectiva persoana are nevoie pentru indeplinirea responsabilitatilor care i-au fost alocate.

Formularul completat trebuie semnat atat de catre utilizator cat si de catre superiorul direct si trebuie transmis Departamentului IT pentru implementare.

Pe baza formularului completat si a aprobarii sale, Departamentul IT va crea conturile solicitate intocmai cu drepturile si profilele specificate.

### 4.4.2. Modificarea conturilor de utilizatori

In cazul in care este nevoie de a modifica un cont de acces in sistemele informatice CertDigital, utilizatorul solicitant va completa un formular de modificare a unui cont de utilizator prin specificarea in detaliu a noilor drepturi pe care le solicita (aplicatii si sisteme informatice, profil de utilizator etc.) dar si a drepturilor pe care le detine si care trebuie anulate odata cu modificarea pozitiei in cadrul CertDigital.

Formularul completat este aprobat de catre superiorul direct al angajatului care isi va exprima acordul si va revizui unde este cazul detaliile privind conturile de utilizator solicitate, dar si a celor care vor fi anulate.

Pe baza formularului completat si a aprobarii sale, Departamentul IT va executa operatiile de modificare a conturile in conformitate cu detaliile specificate.

De asemenea, in cazul intreruperii activitatii pentru o perioada mai lunga de 60 de zile (de exemplu in cazul unui concediu de maternitate), angajatul respectiv are obligatia de a solicita prin formularul pentru modificarea unui cont de utilizator

dezactivarea temporara a contului de utilizator. Formularul trebuie semnat de catre superiorul direct si trimis Departamentului IT care va actiona in consecinta.

### 4.4.3. Dezactivarea conturilor de utilizatori

Procesul de dezactivare a unui cont de utilizator se realizeaza pe baza fisei de lichidare emise de catre Departamentul de Resurse Umane. Astfel, in momentul terminarii contractului de munca cu CertDigital, angajatul respectiv va prezenta Departamentului IT fisa de lichidare care va contine o referire la dezactivarea conturilor sale de utilizator.

Departamentul IT va dezactiva conturile imediat sau in cel mai scurt timp posibil in vederea diminuarii riscului de mentinere a unui cont activ in mod necorespunzator si va confirma acest lucru prin semnarea fisei de lichidare.

Pentru a facilita trasabilitatea activitatilor efectuate cu ajutorul conturilor de utilizator, aceastea vor fi dezactivate si nu sterse. Dupa trecerea unei perioade de minim 24 de luni de la dezactivare, Departamentul IT poate decide stergerea definitiva a conturilor.

## 4.5. Procedura de administrare a utilizatorilor cu drepturi privilegiate

Un drept privilegiat reprezinta accesul nerestrictionat de controalele implementate al unui utilizator la una sau mai multe functionalitati din cadrul unui sistem informatic.

Aceste drepturi includ, dar nu se limiteaza la:

- Un utilizator cu drepturi de administrator;
- Dreptul de accesa direct bazele de date ale aplicaţiilor;
- Drept de acces pe facilitati de sistem specifice (aplicaţii, utilitare).

Alocarea drepturilor privilegiate pentru utilizatori in aplicatiile informatice din cadrul Companiei este permis doar in baza unei autorizatii si a unei nevoi justificate in fişa postului in cazul angajatilor, respectiv in contractele de servicii/ colaborare in cazul terţelor parţi.

Beneficiarii drepturilor privilegiate sunt, in general, administratorii de sisteme, administratorii de reţea, inginerii de sistem sau consultanţii din partea unor terţe

parţi care necesita acces in aplicatiile informatice din cadrul CertDigital pentru a intreprinde actiuni specifice (precum intreţinere, mentenanţa, debugging etc.).

Drepturile privilegiate sunt identificate pentru fiecare element al infrastructurii (de ezemplu sistem de operare, baza de date, etc.) şi pentru fiecare aplicatie. De asemenea, sunt identificate si categoriile de utilizatori pentru care vor fi alocate aceste drepturi.

Anumite situatii de urgenta pot justifica folosirea conturilor privilegiate. Astfel, este efectuata o configurare prealabila a accesului cu drepturi privilegiate si impunerea unui control adecvat. Spre exemplu, datele de acces ale conturilor de utilizatori pot fi pastrate intr-un plic sigilat intr-o locaţie sigura, alaturi de o lista cu persoane autorizate sa foloseasca in caz de necesitate aceste conturi. De asemenea, in plicul sigilat sunt incluse si datele de contact ale administratorului de sistem care trebuie contactat atunci când este necesara deschiderea plicului.

### 4.5.1. Administrarea conturilor de utilizatori cu drepturi privilegiate

Personalul de administrare a aplicatiilor are in responsabilitate crearea, modificarea si dezactivarea conturilor de utilizatori cu drepturi privilegiate. Procesul de creare a unui cont cu drepturi privilegiate pe baza unei cereri emise implica, in plus fata de procesul obisnuit si descris in procedura de administrare a conturilor in sistemele CertDigital.

Conturile de utilizatori privilegiate trebuie permanent revizuite de catre Responsabilul de Securitate pentru a preintâmpina situatia in care ar putea exista in sistem conturi active nefolosite sau drepturi de acces acordate necorespunzator.

Personalul de administrare a sistemului, daca este posibil, nu trebuie sa foloseasca conturile cu drepturi privilegiate pentru desfasurarea activitatilor zilnice de nivel scazut. Pentru aceste activitati, fiecare administrator trebuie sa detina in paralel un cont cu drepturi normale de acces.

### 4.5.2. Monitorizarea conturilor de utilizatori cu drepturi privilegiate

Toate activitaţile desfaşurate prin intermediul unor conturi de utilizator cu drepturi privilegiate vor fi monitorizate si inregistrate. Conform politicii de retentie, aceste fisiere vor fi salvate şi pastrate pentru o perioada determinata de timp şi vor fi

revizuite periodic sau ori de câte ori este nevoie de catre Responsabilul de Securitate. Acesta va intocmi rapoarte regulate conţinând rezultatele procesului de revizuire.

## 4.6. Procedura de management al parolelor pentru personalul CertDigital

Scopul acestei proceduri este de a stabili standarde de creare a parolelor, de protectie si de schimbare frecventa a acestora, astfel incat sistemul informatic CertDigital sa fie protejat impotriva accesului neautorizat.

Parolele sunt asociate cu conturile de utilizator si sunt folosite in cadrul aplicatiilor sau diverselor sisteme CertDigital (de ex. pentru acces la retea, e-mail etc.). De aceea, este necesar ca toti angajatii sa cunoasca recomandarile cu privire la alegerea unor parole adecvate.

### 4.6.1. Reguli privind alegerea parolelor

Parolele **adecvate** au urmatoarele caracteristici:

- Contin atat majuscule cat si litere mici (a-z, A-Z);
- Contin cifre si cel putin un caracter alfanumeric (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Nu sunt cuvinte intalnite in nicio limba, dialect, argou, jargon etc;
- Nu se bazeaza pe informatii personale precum nume, numere de telefon etc;
- Nu coincid si nu contin numele de utilizator;
- Au lungimea minima de opt caractere.

Parolele **neadecvate** reprezinta parole cu grad scazut de complexitate ce sunt deseori caracterizate de una dintre urmatoarele specificatii:

- Reprezinta un cuvant folosit in mod uzual, cum ar fi:
  - Cuvintele „CertDigital”, “Bucuresti”, “parola” sau alte derivate;
  - Numele utilizatorului familie, al copiilor, colegilor de serviciu, animalelor de companie, etc.;
  - Zile de nastere, adrese, numere de telefon, numarul de la masina sau alte informatii personale;

- Cuvinte sau succesiuni de litere sau cifre de genul: abcdef, 123456, zyxwvuts, 123321 etc.;
- Oricare dintre cuvintele de mai sus scrise in ordine inversa;

- Au in alcatuire cuvinte ce se regasesc intr-un dictionar (Roman, Englez etc);
- Coincid sau contin numele de utilizator;
- Au lungimea mai mica de opt caractere.

### 4.6.2. Protejarea parolelor de catre utilizatori

Parolele asociate conturilor de utilizatori nu sunt folosite pentru autentificarea in sisteme externe CertDigital (de exemplu, conturi personale de e-mail, conturi pe site-uri comerciale etc.). De asemenea, parolele sunt alese in mod distinct pentru fiecare tip de aplicatie care necesita autentificare prin parola.

Toate parolele sunt clasificate ca informatii confidentiale si nu este permisa stocarea acestora in sistemele informatice sau pe un alt suport.

In cazul in care controalele referitoare la folosirea parolelor nu sunt respectate, CertDigital adopta masurile adecvate in acest sens pentru a se ajunge la conformitatea cu acestea.

## 4.7. Procedura de utilizare a postei electronice

Pentru a determina cresterea performantelor, Autoritatea de Certificare CertDigital favorizeaza utilizarea mijloacelor electronice de comunicatie (Internet, telefon, pager, mesaje vocale, mesaje electronice si fax).

Toate mesajele emise/ manipulate prin intermediul sistemelor electronice CertDigital sunt considerate proprietatea acesteia cu exceptia situatiilor in care tertele parti isi exprima in mod clar drepturile de autor sau altfel de drepturi de acest gen asupra mesajelor electronice care au trecut prin sistemele electronice enuntate anterior.

Administrarea sistemului de e-mail se realizeaza doar de catre angajatii Departamentului IT.

Administrarea casutelor de e-mail se va realiza tinand cont de procedurile interne ale Companiei.

### 4.7.1. Reguli privind utilizarea postei electronice

Utilizarea sistemului de mesagerie electronica CertDigital trebuie realizata ca parte a activitatii profesionale ce are ca scop imbunatatirea activitatilor de zi cu zi prin inlesnirea comunicarii interne in cadrul CertDigital, respectiv in exterior prin mentinerea legaturilor cu clientii, partenerii de afaceri ai CertDigital sau cu autoritatile locale.

Comunicarea electronica se va limita la materialele care au legatura cu activitatile profesionale si sarcinile de serviciu ale angajatilor si nu va fi folosita ca suport pentru campanii caritabile de strangere de fonduri, campanii de sustinere politica/ religioasa sau pentru activitati ce tin de afaceri personale, amuzament sau distactie.

Aceasta procedura interzice folosirea sistemelor publice de posta electronica pentru trimiterea mesajelor cu privire la activitatile CertDigital.

Este interzisa folosirea de catre un utilizator a unei adrese de e-mail ce apartine altei persoane.

In formularea mesajelor electronice, utilizatorul este obligat sa-si precizeze datele de identificare care trebuie sa reflecte numele acestuia, numarul de telefon, adresa de e-mail sau apartenenta la o anumita organizatie (exceptie fac liniile de tip "hot-line" care sunt, in general, anonime). De asemenea, se recomanda atasarea unei semnaturi electronice in cadrul mesajelor care sa contina informatii despre expeditor precum: pozitia ocupata in cadrul CertDigital, apartenenta la aceasta, adresa etc.

Periodic, angajatii sunt infomati si instruiti sa foloseasca in mod adecvat resursele sistemului informatic al Companiei.

In cadrul comunicatiei electronice, se interzice inlocuirea, inlaturarea sau denaturarea identitatii unui utilizator.

### 4.7.2. Reguli privind continutul mesajelor

Folosirea unor remarci peiorative sau adresarea prin cuvinte obscene in cadrul discutiilor prin intermediul e-mail-urilor cu alti angajati, clienti, competitori sau alte persoane este strict interzisa, deoarece pot sta la baza unor probleme legale ce ar putea determina defaimarea CertDigital. Aceste remarci, ulterior, pot fi

desprinse din contextul initial si folosite impotriva CertDigital. In aceste conditii, pentru a se evita asemenea probleme, angajatii vor trebui sa se rezume in cadrul comunicatiilor electronice doar la comunicarea problemelor de afaceri ale CertDigital in conformitate cu standardele conventionale de etica si buna cuviinta.

## 4.8. Procedura de securitate a informatiilor

Pentru manipularea optima a informatiei, pentru simplificarea deciziilor privind securitatea informatiilor si pentru minimizarea costurilor legate de securitatea informatiilor CertDigital are implementata o ierarhizare a informatiei pe baza confidentialitatii. Principalul scop al acestei ierarhizari este de a furniza un proces consistent de manipulare a informatiilor, indiferent de modul in care se prezinta informatia, cui ii este adresata sau cine o are in custodie.

Fiecare angajat trebuie sa aiba acces doar la informatia necesara pentru a-si indeplini sarcinile de serviciu. Informatiile sensibile trebuie accesate doar de catre angajatii carora proprietarul aplicatiei respective le-a acordat drept de acces.

Informatiile CertDigital nu trebuie folosite in alte scopuri decat cele de business aprobate in mod oficial de catre Conducere. Folosirea neaprobata a informatiilor restrictionate este interzisa. Politica se aplica tuturor tipurilor de informatii cadrul CertDigital. Politica se aplica tuturor partilor care intra in contact cu informatiile CertDigital, inclusiv colaboratorilor externi.

Utilizatorilor nu le este permis sa efectueze nicio activitate in sistemele informatice interne ce ar putea conduce la deteriorarea imaginii CertDigital.

CertDigital foloseste trei categorii de clasificare a informatiilor detaliate in continuare.

### 4.8.1. Informatie Publica

Aceasta informatie este aprobata de catre Conducerea CertDigital ca fiind publica. Dezvaluirea neautorizata a informatiilor publice este admisa intrucat nu poate cauza probleme companiei CertDigital, clientilor sau partenerilor de afaceri. (exemplu de informatie publica brosurile si materialele de pe pagina de internet oficiala). Pentru ca informatia sa fie clasificata ca publica trebuie sa fie etichetata ca atare sub permisiunea Proprietarului Informatiei.

### 4.8.2. Informatie cu utilizare Interna

Utilizarea acestor informatii este permisa in cadrul CertDigital, iar in unele situatii si in cadrul organizatiilor afiliate (partenerilor CertDigital). Dezvaluirea neautorizata a acestui tip de informatii catre persoane din afara CertDigital nu este admisa si poate cauza probleme in cadrul organizatiei, clientilor sau partenerilor de afaceri. Acest tip de informatie poate fi raspandita in interiorul CertDigital fara aprobarea in avans a Proprietarului informatiei. (exemple de informatie cu utilizare interna: numerele de telefon cadrul CertDigital si adresele casutelor de e-mail).

### 4.8.3. Informatie restrictionata

Reprezinta informatia cea mai sensibila si necesita monitorizare permanenta. Se incadreaza la cel mai ridicat nivel de confidentialitate. Divulgarea neautorizata a acestui tip de informatie catre angajatii carora nu le este necesara poate constitui o incalcare a legislatiei si a reglementarilor in vigoare, si poate cauza probleme organizatiei, clientilor sau partenerilor de afaceri. Proprietarul informatiei poate aproba accesul la acest tip de informatii. (exemple de informatie restrictionata: contracte, strategii de business, informatii legale protejate de confidentialitatea avocat-client etc.).

## 4.9. Procedura de personal

### 4.9.1. Cerinţe privind trecutul, calificarile, experienţa şi acceptarea

Personalul care este nominalizat pentru a face parte din echipa care se ocupa cu emiterea/revocarea certificatelor calificate si a marcilor temporare trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.

### 4.9.2. Proceduri de verificare a trecutului

CertDigital face urmatoarele verificari asupra trecutului personalului care se va ocupa cu emiterea/revocarea certificatelor calificate si a marcilor temporare:

- Confirmarea locului de munca anterior;

- Verificarea referinţelor profesionale;
- Confirmarea celei mai inalte sau relevante instituţii de invaţamânt urmate;
- Studierea cazierului judiciar
- Cautarea rapoartelor financiare;
- Cautarea rapoartelor privind permisul de conducere;
- Cautarea rapoartelor privind asistenţa sociala;

In masura in care, oricare dintre cerinţele impuse nu poate fi satisfacuta, CertDigital va folosi o tehnica de investigaţie care este permisa de lege şi care furnizeaza informaţii asemanatoare.

Factorii implicaţi in verificarea trecutului, ce pot duce la respingerea persoanelor candidate a face parte din echipa sau la luarea de masuri impotriva celor care fac parte din echipa, includ:

- Prezentarea greşita facuta de catre candidat;
- Referinţe personale nefavorabile sau care nu inspira incredere;
- Condamnari;
- Indicii ale lipsei de responsabilitate financiara.

Rapoartele care conţin astfel de informaţii sunt evaluate de personalul de la resurse umane şi securitate, care determina cursul potrivit al acţiunii, in funcţie de tipul, importanţa şi frecvenţa comportamentului dezvaluit de verificarea trecutului. Aceste acţiuni pot include masuri care pot ajunge la incheierea rapoartelor contractuale cu persoana respectiva. Folosirea informaţiilor gasite prin verificarea trecutului pentru a intreprinde astfel de acţiuni este supusa legilor aflate in vigoare.

### 4.9.3. Cerinţe de pregatire

CertDigital asigura personalului pregatirea necesara pentru a indeplini in mod competent şi satisfacator responsabilitaţile funcţiei. Programele de pregatire ale CertDigital sunt realizate ţinând cont de responsabilitaţile individuale şi includ urmatoarele:

- Concepte de baza despre infrastructura cheii publice;

- Responsabilitaţile funcţiei;
- Politicile şi procedurile de securitate şi operaţionale CertDigital;
- Folosirea şi funcţionarea hardware-ului şi software-ului existent;
- Raportarea şi tratarea cazurilor de incident şi compromis;
- Procedurile de recuperare in caz de dezastru şi de continuare a activitaţii.

### 4.9.4. Cerinţele şi frecvenţa cursurilor de perfecţionare

CertDigital furnizeaza cursuri de perfecţionare şi de actualizare pentru personal, in masura şi cu frecvenţa care permit asigurarea menţinerii nivelului necesar pentru indeplinirea competenta şi satisfacatoare a responsabilitaţilor de serviciu. Se asigura periodic pregatire de securitate.

### 4.9.5. Sancţiuni pentru acţiuni neautorizate

Se iau masuri disciplinare adecvate pentru acţiunile neautorizate sau pentru alte violari ale politicilor şi procedurilor CertDigital. Acţiunile disciplinare pot include masuri care duc pâna la incheiere contractului şi sunt luate in funcţie de frecvenţa şi severitatea acţiunilor.

### 4.9.6. Cerinţe pentru contractarea personalului

In circumstanţe limitate, se pot folosi contractanţi sau consultanţi independenţi pentru a ocupa funcţii de incredere. Orice astfel de contractant sau consultant este menţinut dupa aceleaşi criterii funcţionale şi de securitate care se aplica şi in cazul CertDigital, care se afla intr-o poziţie asemanatoare. Contractanţii şi consultanţii independenţi care nu au desavârşit procedurile de verificare a trecutului specificate la punctul 4.9.2 pot accesa locaţiile securizate ale CertDigital numai daca sunt escortaţi şi supravegheaţi direct de persoane de incredere.

### 4.9.7. Documentaţie furnizata personalului

Personalul CertDigital implicat in funcţionarea serviciilor infrastructurii cheii publice ale CertDigital trebuie sa citeasca politicile si procedurie operationale si de securitate interne. CertDigital ofera angajaţilor sai pregatirea necesara şi alta

documentaţie necesara pentru a indeplini competent şi satisfacator responsabilitaţile funcţiei.

# 5. Controale privind securitatea informației

## 5.1. Generarea si folosirea perechii de chei

### 5.1.1. Generarea perechii de chei

Procesul de generare a perechilor de chei in cadrul Autoritatii de Certificare CertDigital este realizat de catre persoane de incredere folosind sisteme de incredere si procese care includ in cadrul perechilor de chei securitatea si structura criptografica necesara.

Sistemul hardware de criptografie folosit pentru generararea perechilor de chei indeplineste cerintele standardului NIST FIPS 140-2 Nivel 3.

Toate activitatile de generare de chei intreprinse sunt inregistrate, datate si semnate de catre toate persoanele implicate. Documentele justificative aferente proceselor de generare a cheilor si altor operatiuni sensibile sunt stocate si puse la dispozitia auditorilor pentru revizuiri ulterioare.

### 5.1.2. Functiile hash si algoritmii criptografici utilizați

În conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS), Legea nr. 214/2024 și standardele ETSI aplicabile (ex. ETSI EN 319 401, ETSI EN 319 412, ETSI TS 119 312/512), Autoritatea de Certificare CertDigital utilizează doar primitive criptografice considerate sigure la data prezentei și prevăzute în Politica criptografică a furnizorului, după cum urmează:

**a) Funcții hash acceptate**

- SHA-256 (minim), SHA-384 și SHA-512;

- algoritmi depășiți precum **SHA-1** sau **MD5 nu sunt acceptați**.

**b) Algoritmi de semnătură digitală**

- RSA cu dimensiunea cheii ≥ 2048 biți (recomandat 3072/4096);

- ECDSA pe curbele NIST P-256 / P-384 / P-521;

- EdDSA (ex. Ed25519 / Ed448), acolo unde este prevăzut de politicile/profilurile de certificat.

**c) Servicii de marcare temporală (QTSA)**

- semnături TSA emise, de regulă, cu RSA 3072/4096 și SHA-256/512, în funcție de politica TSA activă;

- sincronizare timp trasabilă la UTC și menținerea integrității lanțurilor de timp conform ETSI TS 319 421/422.

**d) Parametri și lungimi de chei**

Sunt stabiliți în Politica criptografică și pot fi actualizați în funcție de recomandările ETSI/ENISA și de starea științei.

**e) Mecanism de actualizare (crypto-agility)**

- CertDigital își actualizează setul de algoritmi/parametri atunci când apar vulnerabilități sau la atingerea termenelor de viață criptografică;

- documentele și dovezile existente sunt re-augmentate pentru menținerea verificabilității pe termen lung (ex. profiluri AdES-LTA/ERS).

### 5.1.3. Livrarea cheii private

In cazul in care cheile unui utilizator au fost generate de catre Autoritatea de Certificare, livrarea acestora catre utilizator se realizeaza in doua modalitati:

- Sunt livrate personal prin stocarea pe un dispozitiv criptografic (de exemplu, token), sau in anumite cazuri, in format PKCS#1;
- Prin scrisoare poştala recomandata.

Informatiile necesare decriptarii cheilor sau de activare a cardului (codul PIN) sau (parola) sunt furnizate in mod separat de mediul de stocare care conţine perechile de chei.

### 5.1.4. Livrarea cheii publice catre emitentul certificatului

Semnatarul trimite emitentului de certificat cheia publica generata printr-o cerere electronica intr-o sesiune securizata SSL care respecta sintaxa standard pentru cererile de certificat PKCS#10.

Livrarea cheii publice are loc in aceeași sesiune cu furnizarea detaliilor de catre solicitant in cadrul cererii de emitere a certificatului.

### 5.1.5. Livrarea cheii publice către utilizatori

In conformitate cu standardul X.509 Versiune 3, CertDigital distribuie cheile publice sub forma de certificate prin intermediul serviciilor de posta electronica sau a site-ului CertDigital prin descarcare.

### 5.1.6. Dimensiunile cheii

Perechile de chei ale Autoritatii de Certificare CertDigital sunt definite pe 4096 biti, iar cele destinate utilizatorilor sunt definite pe 2048 biti.

### 5.1.7. Generarea cheii hardware/software

Perechile de chei ale abonatilor sunt generate si stocate in infrastructura hardware si software. Este recomandat ca abonatii sa utilizeze un modul criptografic NIST FIPS 140-2 Nivel 3 pentru generarea cheilor.

## 5.2. Protectia cheilor private

### 5.2.1. Standarde pentru modulele criptografice

CertDigital foloseste module criptografice care sunt certificate FIPS 140-2 Nivel 3 si indeplinesc standardele industriale pentru generarea de numere aleatorii.

Cheile utilizate de catre Autoritatea de Certificarea CertDigital sunt generate si stocate in module de securitate hardware (HSM) ce pot fi activate simultan doar de doua persoane, si care, de asemenea, este validat NIST FIPS 140-2 Nivel 3.

In functie de starea in care se afla, o cheie (publica sau privata) poate fi incadrata intr-una dintre urmatoarele faze:

- „*In asteptare*” – cheia este generata, dar nu esta lansata in perioada de valabilitate;
- „*Activa*” – cheia este utilizabila complet din punct de vedere al functionalitatilor;

- „*Expirata*” – perioada de valabilitate a cheii este depășita. Cheia poate fi folosita doar pentru validarea semnaturilor electronice, nu si pentru creare.

### 5.2.2. Controlul multi-persoane al accesului cheii private

Serviciile CertDigital folosesc module hardware care necesita implicarea mai multor pesoane pentru a indeplini sarcini sensibile. Toate instrumentele necesare realizarii acestori operatiuni sunt stocate in siguranta si nu pot fi accesate fara informatiile detinute de catre persoanele autorizate.

### 5.2.3. Back-up-ul cheilor private

Cheile private CertDigital sunt generate si stocate in cadrul unui modul hardware critptografic. In cazul in care aceste chei trebuie transferate pe alte medii in scopul realizarii unui back-up, acestea sunt transferate si stocate intr-o forma criptata pe echipamente specializate de stocare a cheilor.

### 5.2.4. Arhivarea cheilor private

Autoritatea de Certificare CertDigital nu stocheaza in mod normal copii ale cheilor private ale utilizatorilor de certificate. Crearea acestor copii se realizeaza numai la solicitarea utilizatorilor.

### 5.2.5. Intrarea unei chei private in modulul criptografic

Cheile private CertDigital se genereaza si se stocheaza pe modulele de securitate hardware validate FIPS 140-2 Nivel 3, in care, de altfel, vor fi folosite.

Transferul cheilor private in exterior se realizeaza numai in forme criptate.

### 5.2.6. Activarea cheilor private

Activarea cheilor private aferente certificatelor calificate CertDigital emise presupune autentificarea prin parola si/ sau PIN.

Utilizatorii sunt singurii responsabili pentru protectia cheilor private pe care le au in posesie. CertDigital nu detine nicio responsabilitate in generarea, protejarea sau distribuirea acestor chei.

CertDigital sugereaza utilizatorilor sai autentificarea folosirea parole puternice pentru a preintampina accesul neautorizat si folosirea frauduloasa a cheilor private.

### 5.2.7. Dezactivarea cheilor private

Cheile private stocate pe un modul de securitate hardware sunt dezactivate odata cu scoaterea cardului din dispozitiv.

In cazul unui utilizator, dezactivarea cheii primare se realizeaza la iesirea din aplicatia, cand, de fapt, se inchide sesiunea de lucru.

In timpul utilizarii, modulele de securitate hardware nu trebuie lasate nesupravegheate sau in oricare alta stare care ar putea favoriza accesul neautorizat. Cand nu sunt folosite, modulele trebuie depozitate intr-o locatie incuiata ce beneficiaza de un grad sporit de securitate.

### 5.2.8. Distrugerea cheii private

In forma initiala, distrugerea cheii primare presupune stergerea ei de pe mediul de stocare intr-o maniera care sa asigure faptul ca nu au ramas fragmente ale cheii care ar putea permite reconstituirea ei.

Modulele de Securitate Hardware (primare si cele de back-up) sunt reinitializate in conformitate cu specificatiile producatorului de hardware. In cazul in care, aceasta procedura esueaza, CertDigital isi asuma obligatia de a distruge echipamentele intr-o mod care sa nu permita recuperarea cheii private.

### 5.2.9. Formatul documentelor ce pot fi semnate electronic

Serviciile de certificare furnizate de catre CertDigital permit folosirea semnaturii pentru orice tip de document electronic.

Spre exemplu, daca documentul ce trebuie semnat este un format PDF, atunci va rezulta tot un format PDF, acesta avand o structura de tip XML ce permite includerea in fisier a semnaturilor electronice.

Pentru orice alt fisier va fi generat un fisier anvelopa, ce va include fisierul vechi si semnaturile. Acest fisier va avea extensia P7M (PKCS#7 Message).

## 5.3. Alte aspecte privind managementul perechilor de chei

### 5.3.1. Arhivarea cheilor publice

Certificatele CertDigital emise către utilizatori sunt stocate in depozitarul de certificate si pe medii de rezerva.

### 5.3.2. Perioada de utilizare a cheilor private si publice

Certificatele emise de CertDigital si perechile de chei corespunzătoare pot fi folosite pe toata perioada de valabilitate in cazul in care nu apar încălcări ale regulamentelor care sa necesite revocare imediata.

In cazul cheilor private si publice, expirarea perioadei de valabilitate determina restrângerea funcționalităților la nivel de decriptare (in cazul cheilor private), respect de verificare a semnăturii in cazul cheilor publice.

Valabilitatea certificatelor CertDigital se structurează după cum urmează:

| **Certificat emis de:** | **Valabilitate:** |
|---|---|
| Autoritate de certificare ROOT | 35 ani |
| Subautoritati | 15 ani |
| Autoritate de certificare pentru utilizatori | 1 an, doi sau 3 ani |

In cadrul unor eventuale litigii, pentru a putea face dovada certificarii, informatiile cu privire la un certificat calificat sunt pastrate pentru o perioada de minim 10 ani de la data incetarii valabilitatii certificatului.

## 5.4. Datele de activare

### 5.4.1. Instalarea si generarea datelor de activare

Pentru activarea modulului de securitate hardware, personalul CertDigital si utilizatorii serviciilor sunt instruiti sa foloseasca parole de autentificare puternice.

Angajatii CertDigital stabilesc parole in conformitate cu prevederile procedurii de administrare a parolelor descrise in cadrul acestui document.

### 5.4.2. Protectia datelor de activare

Angajatii CertDigital sunt instruiti sa nu divulge parolele strainilor si sa nu-si noteze parolele pe medii care ar putea fi accesibile altor persoane.

## 5.5. Controalele de securitate ale statiilor de calcul

Serverele si echipamentele de calcul din cadrul CertDigital ruleaza pe sisteme de incredere configurate si testate folosind cele mai bune practici in domeniu. Toate sistemele de operare necesita identificare individuala si restrictii de acces la serviciile de control bazate pe autentificarea identitatii.

Sistemele sunt scanate pentru detectia programelor cu caracter malitios si, de asemenea, sunt protejate impotriva programelor de tip spyware sau virus.

Reteaua CertDigital este prevazuta cu solutii de firewall pentru protectia impotriva tentativelor de intruziune din interior sau exterior si pentru limitarea proceselor din retea, care ar putea produce vulnerabilitati in sistemele de productie.

## 5.6. Controale tehnice privind ciclul de viata

### 5.6.1. Controale specifice dezvoltarii sistemului

Implementarea sistemelor in cadrul CertDigital se realizeaza in conformitate cu standardele actuale privind dezvoltarea sistemelor si administrarea schimbarilor.

Inainte de a fi lansate in mediul de productie, rezultatele implementarii modificarilor sunt testate intr-un mediu de test.

Procesul de testare este derulat de catre personalul IT si reprezentantii utilizatorilor finali ai aplicatiilor din cadrul departamentelor care folosesc sistemul care a fost modificat.

Testarea se realizeaza pe baza unor scenarii de testare predefinite, care includ printre altele persoanele responsabile de testare, durata de desfasurare a testelor, datele de test, etc.

Daca este aplicabil, se vor efectua urmatoarele tipuri de teste:

- Testare functionala;
- Teste de Integrare;

- Testare de Acceptanta din partea Utilizatorilor - UAT

Datele de testare nu vor fi folosite in mediul de productie, iar datele din mediul de productie se vor putea utiliza in testare decat daca au fost depersonalizate.

### 5.6.2. Controale de management al securitatii

CertDigital implementeaza controale de management al securitatii pentru a asigura o functionalitate optima a sistemelor informatice, si implicit de a garanta functionarea in conformitate cu cerintele operationale.

CertDigital a implementat in cadrul sistemelor IT controale ce permit verificarea permanenta a integritatii si disponibilitatii sistemelor din punct de vedere hardware si software.

## 5.7. Controale de securitate in retea

Infrastructura IT CertDigital beneficiaza de sisteme de protectie atat la nivel intern cat si la nivel extern prin folosirea unor solutii de firewall si a unor sisteme de detectie a intruziunilor.

Accesul utilizatorilor in sistemele CertDigital este permis direct doar pentru procesele care au o stransa legatura cu activitatea pe care o desfasoara.

# 6. Profilele certificatelor si Lista Certificatelor Revocate

## 6.1. Profilele certificatelor

Profilele certificatelor emise de CertDigital respecta standardul X.509 versiunea 3.

In conformitate cu acest standard, structura unui certificat se constituie din:

- corpul certificatului;
- informatii despre algoritmul folosit pentru semnarea certificatului;
- semnatura electronica propriu-zisa a Autoritatii de Certificare.

### 6.1.1. Continut

Campurile de baza ale unui certificat CertDigital sunt:

| Camp | Valoare sau valoare obligatorie |
|---|---|
| Versiune | X.509 Versiunea 3 |
| Numar de serie | Valoare unica aferenta certificatelor CertDigital emise |
| Algoritm de semnatura | Obiect identificator al algoritmului utilizat pentru semnarea certificatului (functia hash-code SHA256/SHA512 si algoritmul de criptare RSA) |
| Emitent ND | Autoritatea emitenta a certificatului |
| Valabil incepand cu | Data de incepere a validitatii certificatului identificata pe baza sincronizarii serverului cu ora oficiala a Romania |
| Valabil pana la | Data de expirare a validitatii certificatului identificata pe baza sincronizarii serverului cu ora oficiala a Romaniei. Valabilitatea certificatelor se stabileste in concordanta cu |

| | |
|---|---|
| | prevederile obligatorii. |
| Subiect (Nume Distinct) | Numele distinctiv respecta cerintele standardului X.509 v.3. Anumite atribute din componenta Numelui Distinct pot avea caracter optional. |
| Subiectul cheii publice | Codificat in conformitate cu RFC 3280 |
| Semnatura | Generata si codificata in concordanta cu RFC 3280 |

### 6.1.2. Numarul de versiune

Certificatele Autoritatii de Certificare CertDigital şi ale utilizatori finali sunt certificate emise respectand standardul X.509 versiunea 3.

### 6.1.3. Extensii

In concordanta cu standardul X.509 versiunea 3, certificatele emise de catre CertDigital includ urmatoarele campuri de extensie:

| Camp de extensie | Semnificatie |
|---|---|
| **basicConstraints** | Extensie critica cu valoare falsa |
| **keyUsage** | Extensie critica cu valoarea digitalSignature, keyEncipherment |
| **subjectAltName** | Extensie non-critica prin care se ataseaza la subiectul certificatului o identitate aditionala (de exemplu, o adresa de e-mail) |
| **authorityKeyIdentifier** | Extensie non-critica prin care se identifica certificatul Autoritatii de Certificare necesar pentru verificarea unui certificat emis |

| | |
|---|---|
| **qcStatements** | Extensie non-critica prin care se indica faptul ca certificatul emis este un certificat calificat |

### 6.1.4. Identificatorul algoritmului de semnare

Identificatorul *(„Algoritm de semnătură”*) din certificat indică algoritmul criptografic efectiv folosit la semnarea electronică a certificatului (ex.: sha256WithRSAEncryption, ecdsa-with-SHA384).

În conformitate cu Regulamentul (UE) 910/2014 (eIDAS), Legea nr. 214/2024 și standardele ETSI aplicabile, Autoritatea de Certificare CertDigital utilizează numai primitive criptografice acceptate în prezent, după cum urmează:

- Funcții hash acceptate: SHA-256, SHA-384, SHA-512 (algoritmi depășiți precum SHA-1/MD5 nu sunt utilizați).
- Algoritmi de semnătură: RSA (chei ≥ 2048 biți, recomandat 3072/4096, cu perechi sha256/384/512WithRSAEncryption), ECDSA pe P-256/P-384/P-521 (ex. ecdsa-with-SHA256/384/512) și, unde este prevăzut, EdDSA (ex. Ed25519/Ed448).

Parametrii și lungimile de chei sunt definiți în Politica criptografică a CertDigital și pot fi actualizați (crypto-agility) în funcție de recomandările ETSI/ENISA.

Dovezile existente pot fi re-augmentate pentru a menține verificabilitatea pe termen lung (ex.: profiluri AdES-LTA).

### 6.1.5. Campul ce specifica semnatura elecronica

Valoarea corespunzatoare campului *Semnatura* se obtine prin aplicarea functiei de hash asupra campurilor certificatului.

## 6.2. Profilul Listei de Certificate Revocate

Listele certificatelor revocate respecta standardul X.509 versiunea 3.

In concordanta cu acest standard, structura unei liste se constituie trei tipuri de informatii dupa cum urmeaza:

- informaţii despre certificatele revocate;
- informatii despre identificatorul algoritmului folosit pentru semnarea listei;
- informatii despre semnatura electronica a Autoritatii de Certificare.

### 6.2.1. Continut

Campurile de baza ale unei liste de certificate revocate sunt:

| Camp | Valoare sau valoare obligatorie |
|---|---|
| **Versiune** | A se vedea sectiunea 7.1.1 |
| **Numarul Listei de Certificate Revocate** | Numar alocat versiunilor de Liste a Certificatelor Revocate |
| **Emitent** | Autoritatea care a semnat si emis Lista Certificatelor Revocate |
| **Data punerii in vigoare** | Data la care au fost emisa o Lista a Certificatelor Revocate. Punerea in vigoarea se realizeaza dupa momentul emiterii |
| **Algoritm de semnatura** | Obiect identificator al algoritmului utilizat pentru semnarea Listei de Certificate Revocate (functia hash-code SHA256/SHA512 si algoritmul de criptare RSA) |
| **Data urmatoarei actualizari** | Data de emitere a urmatoarei Liste de Certificate Revocate |
| **Certificate revocate** | Lista certificatelor revocate, incluzand numarul de serie al certificatelor revocate si data la care au fost revocate. |

### 6.2.2. Numărul de versiune

Listele Certificatelor Revocate emise de către CertDigital respecta standardul X.509 versiunea 3.

# 7. Administrarea documentului

## 7.1. Mecanismul de schimbare

Modificarile care pot surveni in continutul acestui document sunt determinate fie de obtinerea unor neconformitati in urma unor revizuiri ale proceselor fie din imbunatatiri periodice ale fluxurilor operationale in cadrul CertDigital.

Implementarea modificarilor actualizeaza numarul de versiune al documentului si data de emitere a Declaratiei in functie de data la care au fost efectuate modificarile.

Autoritatea de Certificare CertDigital isi aloca dreptul de a efecta modificari de continut (corectarea erorilor de tipar, modificarea legaturilor URL publicate, schimbari in informatiile de contact etc.) asupra practicilor de certificare din acest document.

Revizuirile Declaratiei Practicilor de Certificare fara impact sau cu un impact nesemnificativ asupra semnatarilor si partilor de incredere care utilizeaza certificatele emise de CertDigital si informatiile corespunzatoare legate de starea certificatului se pot realiza si inregistra fara a notifica utilizatorii si partile de incredere si nu implica modificarea numarului de versiune a documentului sau data de intrare in vigoare.

Printre modificarile care impun notificari asupra entitatilor se numara:

- modificari efectuate asupra extensiei pentru un grup de utilizatori de certificate;
- includerea unor tipuri noi de certificate;
- schimbari semnificative de continut si asupra modului de interpretare a campurilor certificatului si ale Listei de Certificate Revocate.

Odata cu sintetizarea modificarilor de implementat, Declaratia Practicilor de Certificare intra in procedura de aprobare interna care se desfasoara pe baza unui comitet format din directorul general, directorul general adjunct si managerii departamentelor tehnice.

Responsabilitatea intretinerii acestui document este alocata catre managerul departamentului care asigura furnizarea serviciilor de certificare. Aferent aprobarii, Declaratia Practicilor de Certificare este transmisa Organismului de Supraveghere urmand ca in termen de 10 zile, sa fie publicat si marcat ca fiind valid.

Versiunea curenta a Declaratiei Practicilor de Certificare este datata ianuarie 2021.

## 7.2. Mecanismul de publicare si notificare

Acest document este disponibil in forma electronica pe site-ul CertDigital la adresa: www.certdigital.ro sau poate fi solicitat prin posta electronica la adresa office@certdigital.ro.

Prin interfata online de afisare a informatiilor public, CertDigital pune la dispozitie doua versiuni ale documentului:

- Versiunea curenta;
- Versiunea anterioara;

Documentele de securitate considerate confidenţiale de catre CertDigital sunt inaccesibile publicului.

## 7.3. Procedura de aprobare a documentului

Declaratia Practicilor de Certificare actualizata este considerata fi valida din momentul publicarii sale pe site-ul CertDigital.

Utilizatorii care nu agreaza varianta actualizata a Declaratiei Practicilor de Certificare si a modificarilor aferente sunt obligati ca in termen de 15 zile de la data validarii noii versiuni, sa intocmeasca o declaratie in acest sens. In acest caz, Autoritatea de Certificare CertDigital isi atribuie dreptul de a rezilia contractul de furnizare a serviciilor de certificare si la revocarea certificatului emis in baza acestuia. Ulterior intervalului de 15 zile de la punea in vigoare a noii versiuni, CertDigital considera ca implicit acceptul utilizatorilor.